privacy and security of communications not authorized to be intercepted[44] with the government's authority to collect CII.[45]

B. Timing Information (Time Stamping)

1. Timing Information Is a Required CII Capability

Timing information is information that distinguishes and properly associates CII with the content of several communications that occur at approximately the same time. A timing information capability would require a carrier to time stamp each CII message within a specific amount of time from when the event triggering the message occurred, and send the CII message to law enforcement within a defined amount of time after the triggering event. Together, this allows law enforcement to associate the CII message with the communication content information (i.e., the communication) and associate the party contacted by the subject with the communication,

The Commission already has held in the *Third R&O* that a timing information requirement is a CII capability required by CALEA Sections 102(2) and 103(a)(2).[46] Specifically, the Commission stated:

> We will adopt a timing information requirement as an assistance capability requirement of section 103 of CALEA.

---

44 *See id.* §§ 1002(a)(4)(A), 1006(b)(2).

45 *See* id. § 1002(a)(2). Although Federal law does not prohibit law enforcement agencies from filtering a broader packet stream and extracting the authorized CII from that stream, implementing a packet activity capability would help alleviate the burden on law enforcement agencies, and at the same time complement CALEA's privacy requirements.

46 *Third R&O* at 16835 ¶ 95.

> First, we find that time stamping is call-identifying information as defined in section 102(2) of CALEA. This information is needed to distinguish and properly associate the call identifying information with the content of several calls occurring at approximately the same time. In other words, time stamp information is needed to identify "the origin, direction, destination, or termination" of any given call and, thus, fits within the statutory definition of section 102(2). Second, we find that delivery of call identifying information, including time stamp information, to the [law enforcement agency] must, pursuant to section 103(a)(2), be provided in such a timely manner to allow that information "to be associated with the communication to which it pertains."[47]

In adopting a timing information requirement, the Commission also adopted specific parameters for delivery of the required timing information. Specifically, a CII message must be transmitted to the law enforcement agency's Collection Function within eight seconds of its receipt by the intercept access point ("IAF") 95% of the time, and with an accuracy within 200 milliseconds.[48] The timing information requirement – including the specific parameters for delivery of the required timing information – was codified in the Commission's rules[49] and remains in force today. As a result of the Commission's conclusions in the *Third R&O* and the adoption of a rule requiring a timing information capability, the timing information (time stamping) capability was

---

47 *Id.*

48 *Id.* at 16835 ¶ 96.

49 47 C.F.R. §§ 64.2202, 64.2203(c) (now contained in 47 C.F.R. §§ 1.20007(a)(14), (b)(5)).

added by industry to J-STD-025-A.[50] As more fully discussed below, there is no reason why this capability should not have been included in J-STD-025-B.

2. The Commission Should Reaffirm That Timing Information (Time Stamping) Is a Required Capability

Despite the requirements of CALEA Section 103(a)(2) and the Commission's directive in the *Third R&O*, J-STD-025-B does not contain language that establishes specific parameters for delivery of the required timing information (time stamping). As a result, unlike its predecessor J-STD-025-A, J-STD-025-B is ambiguous as to whether the Commission's timing requirements for accuracy and delivery of CII apply to packet data services.

J-STD-025-Bs ambiguity over the timing information (time stamping) capability arises from a footnote added to a June 2004 version of J-STD-025-B at the request of an industry representative. The footnote stated that the *Third R&O's* timing "requirement is established by the [Commission] for *circuit-mode only*."[51] Notwithstanding that the Commission's *Third R&O* clearly addressed both circuit-mode and packet-mode communications,[52] certain TIA members took the position – based on the addition of the footnote – that the Commission's time stamping requirement does not apply to any packet data services. Although the footnote subsequently was removed from J-STD-

---

50 See ANSI/J-STD-025-A-2003, § 4.7.

51 Ballot Version of ANSI J-STD-025-B, §§ 3, 4.7 n.2 (June 2004) (emphasis added).

52 *Third RDO* at 16795 ¶ **1.**

025-B, that standard is silent as to whether timing information (time stamping) must be provided, and several TIA members continue to this day to dispute whether the timing requirements set forth in the *Third R&O* apply to packet data services.

The Commission held in the *Third R&O* that circuit- and packet-mode communications services are each subject to CALEA, and adopted capabilities in the *Third R&O* that apply to *both* circuit- and packet-mode services.[53] Given the Commission's holding, it is entirely unclear why certain TIA members continue to maintain that the time stamping requirement does not apply to packet data services. The Commission should make clear that, irrespective of what the standard states, carriers nonetheless must comply with the letter and spirit of the Commission's timing information capability rule.

Although the Commission concluded in the *Third R&O* that J-STD-025 (later J-STD-025-A) was not a sufficient CALEA solution for packet-mode services,[54] the Commission set a September 2001 deadline for packet-mode compliance,[55] and specifically requested that TIA "study CALEA solutions for packet-mode technology and report to the Commission [by September 20001 on steps that can be taken, *including*

---

53 *Id.*

54 *Third R&O* at 19819 ¶ 55. The Commission's conclusion was rooted in its concerns about the technical mechanisms for providing the required capabilities to law enforcement, rather than the required capabilities themselves. See *id.* at 16795 ¶ 1, 16819-20 ¶¶ 55-56.

55 *Id.* at 16819 ¶ 55.

particular amendments to J-STD-025."[56] It is clear from the Commission's statements that such packet-mode compliance would include providing the capabilities adopted in the *Third RDO* via amendments to J-STD-025 – i.e., in J-STD-025-B. Therefore, there is nothing in the *Third R&O* that suggests that the capabilities adopted therein – including the timing information (time stamping) requirement – do not apply to packet-mode (data) services.[57]

Nor is there anything in the *Third R&O* that would preclude the application of the timing information requirements specified therein to packet-mode (data) services. In fact, the Commission's rules contain no distinction about the type of communications (i.e., circuit-mode vs. packet-mode) to which the timing capability applies; the rules state only that "wireline, cellular, and PCS telecommunications carriers shall provide to a [lawenforcement agency] [a timing information capability]."[58]

Highly accurate timing information is critical for a number of important reasons. First, as the Commission recognized, time stamping is critical to proper correlation of the CII events to the associated intercepted communications content stream.[59] The less accurate the time stamp, the greater the possibility that multiple events occurring in the

---

[56] *Id.* (emphasis added); see *also id.* at 16820 ¶ 56. TIA commenced work on the J-STD-025-B packet data standard in direct response to the Commission's directive in the *Third R&O*.

[57] *Third R&O* at 16795 ¶ 1,16819-20 ¶¶ 55-56.

47 C.F.R. § 1.20007(b)(5).

[59] *Third RDO* at 16835 ¶ 95.

same time frame will lead to a misinterpretation of the sequence of CII events.

Second, unlike traditional circuit-switched networks, electronic intercepts in packet data sessions may occur at multiple points (nodes) within a carrier's network. In fact, because of the diffuse nature of packet-based technologies (i.e., that packet data sessions can occur at multiple nodes in a carrier's network and involve multiple IAPs), time stamping is even more critical in the packet-mode communications context than the circuit-mode context. Thus, it is critically important that time stamping occur so that the CII events between these multiple network nodes can be properly correlated with the communications content.

Third, multiple simultaneous packet data sessions can be established by a user of packet-mode services. A time stamp capability is needed to correlate the CII events and communications content on a timeline for each session, and to permit law enforcement to distinguish between CII events for each different session. Moreover, to the extent that two communications sessions may be related, this level of accuracy will allow law enforcement to correlate, where necessary, the two sessions.

Finally, accurate time stamping for packet data intercepts – regardless of the format used to deliver the intercepted communications to law enforcement – is crucial to law enforcement's reconstruction of the sequence of events contained in the interception.

The lack of accurate timing information (time stamping) requirements frustrates CALEA's purpose because it impedes law enforcement's ability accurately to associate

CII with communications content. Indeed, as a practical matter, without accurate time stamping, law enforcement may not be able to correctly determine when the CII events occurred or correlate them with the communications content. As a result, a court order can be frustrated as much as if the information were not delivered to law enforcement at all.

Given that packet mode communications are subject to CALEA,[60] and in light of the Commission's conclusion in the *Third R&O* that timing information is CII under Section 102(2),[61] there is no rational basis for omitting a timing information (time stamping) assistance capability from a packet mode standard such as J-STD-025-B. Indeed, the fact that a time stamping capability is more significant with respect to packet-mode communications should compel its inclusion in such standards.

Therefore, in order to resolve any ambiguity, DOJ requests that the Commission reaffirm that a timing information (time stamping) requirement is applicable to packet data services, regardless of the technology used by the carrier to provide the service. In addition, DOJ asks the Commission to require that carriers provide, at a minimum, a timing information (time stamping) capability that meets the requirements prescribed in the *Third R&O* and codified in the Commission's rules – including the specific

---

60 *Id.* at 16795 ¶ 1.

61 *Id.* at 16835 ¶ 95.

parameters for delivery of the required timing information.[62, 63]

C. Capability to Provide All Reasonably Available Location Information for a Mobile Handset at the Beginning and the End of a Communication[64]

1. Signaling Information That Reveals the Location of a Mobile Handset Is Call-Identifying Information That Is Required to Be Provided Pursuant to Lawful Authorization When It Is Reasonably Available to a Carrier

J-STD-025-B also fails to provide all of the reasonably available CII regarding the location of a mobile handset at the beginning and the end of a communication. The location information capability in J-STD-025-B provides law enforcement only with "cell site" information – i.e., the location of the cellular tower with which a subject's mobile handset is connected – at the beginning and the end of a communication. As a practical

---

62 The 200 millisecond time stamp requirement prescribed in the *Third R&O* (see *Third R&O* at 16835-36 ¶¶ 95-96) is reasonable for industry with respect to packet-mode services because it already is included in various CALEA packet data standards (e.g., ANSI standard T1.678; ANSI standard T1.724; TIA Trial Use Version of J-STD-025-B) and has been deployed by vendors and carriers. Moreover, several equipment manufacturers have stated publicly that the 200 millisecond time stamp requirement is feasible and provided by their equipment. There are also a number of protocols that support time synchronization of up to one (1) millisecond, including the Network Time Protocol (see IETF RFC 1305), Simple Network Time Protocol (see IETF RFC 2030), and the Precise Time Protocol (PTP) (see IEEE 1588).

63 Since a time stamp indicates the date and time that an event is detected in the network, the time stamp also should include the time zone offset from universal coordinated time (UTC). A number of vendors already provide this feature as part of the time stamp capability.

64 The discussion of, and positions regarding, a location information capability for wireless packet data services contained herein relates only to terrestrial use of such services, and does not relate to any potential separate use of such services on board aircraft in an air-to-ground communications services context.

matter, this capability frequently does not provide law enforcement with the information required and intended by CALEA, in terms of both type and accuracy. Many carriers today, moreover, have reasonably available to them additional signaling information that more accurately identifies the location of the mobile handset itself.

CALEA Section 103(a) requires, among other things, that a telecommunications carrier enable law enforcement agencies operating with proper legal authority to (1) intercept wire or electronic communications, and (2) access CII that is reasonably available to the carrier before, during, and immediately after the transmission of wire or electronic communications and in a manner that allows it to be associated with the communication to which it pertains.[65] Thus, Section 103 makes clear that law enforcement agencies are entitled, pursuant to lawful authorization, to receive all CII that is reasonably available to the carrier.

In evaluating the propriety of the particular location capability included in the original J-STD-025 CALEA standard, both the Commission and the D.C. Circuit held that cell site information concerning the location of a mobile handset at the beginning and the end of a communication is CII under CALEA.[66] As both the Commission and

---

65 *See* 47 U.S.C. §§ 1002(a)(1) and (2).

66 *See Third R&O* at 16815 ¶ 44 (finding that "a subject's cell site location at the beginning and end of a call is call-identifying information under CALEA"); *United States Telecom. Ass'n,* 227 F.3d at 463-64. The fact that information indicating the mobile handset location for mobile calls is signaling information that falls within the statutory definition of CII provided further support for the D.C. Circuit's conclusion. See *United States Telecom. Ass'n,* 227 F.3d at 463-64 (holding that the mobile phone signals at the

the D.C. Circuit found, location information at the beginning and the end of a communication identifies the origin or destination of the communication.[67] And as both the Commission and D.C. Circuit recognized, signaling that reveals the location of a mobile handset is CII that CALEA requires carriers to be "capable of . . . expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access" when reasonably available to the carrier.[68]

Signaling information that reveals the location of a mobile handset is indisputably CII. Accordingly, such information is required to be provided to law enforcement agencies pursuant to lawful authorization, where it is reasonably available to a carrier.

2. All Reasonably Available Signaling Information That Reveals the Location of a Mobile Handset Should Be Provided to Law Enforcement Pursuant to Lawful Authorization

CALEA Section 103(a)(2) requires carriers to isolate and enable law enforcement to access pursuant to lawful authorization CII that is reasonably available to the

---

beginning and end of a call necessary to achieve communications between the caller and the called party are signaling information that is call identifying information).

67 *United States Telecom. Ass'n, 227* F.3d at 463. Moreover, the Commission found in the *Third R&O* that at least cell site location information is reasonably available to wireless carriers. *Third RDO* at 16816 ¶ 45 (stating that "location information is reasonably available to cellular and broadband PCS carriers").

68 *See Third RDO* at 16815-16 ¶¶ 44-45. Consistent with the statute, this Petition requests only capabilities to provide information that is reasonably available in carrier's networks.

carrier,[69] and contains only one restriction with respect to the provision of location information to law enforcement: it precludes a carrier from providing – "solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code)" ("PR/TT order") – information that may disclose the physical location of the subscriber, except where location may be determined from the telephone number.[70] The Commission stated in the *Third RDO* that the language in Section 103(a)(2)(B) ". . . does not exclude location information from the category of 'call-identifying information,' but simply imposes on law enforcement an authorization requirement different from that minimally necessary for the use of pen registers and trap and trace devices."[71] The Commission went on to state that its conclusion was justified because ". . . interpreting [Section 103(a)(2)(B)] to exclude location information from the technical requirements for CALEA would render the provision 'mere surplusage' and would thus conflict with the usual rules of statutory construction."[72] In upholding the Commission's conclusions concerning location information,[73] the D.C. Circuit agreed that such a reading was required by the "well-accepted principle of statutory construction that requires every provision of a

---

69 *See* 47 U.S.C. § 1002(a)(2).

70 *See id.* § 1002(a)(2)(B).

71 *Third RDO* at 16815¶ 44.

72 *Third R&O* at 16815 n.95.

73 *See United States Telecom. Ass'n. 227* F.3d at 463

statute to be given effect."[74] Accordingly, CALEA requires that carriers will provide law enforcement access to location information pursuant to Section 103(a)(2) and proper legal authorization except where the government acts "solely pursuant" to a PR/TT order

Moreover, CALEA does not specifically delineate the type(s) of location information to be provided. Rather, the inclusion of the phrase "reasonably available to the carrier" in Section 103(a)(2) recognizes that different carriers could and would provide different location information based on availability in their respective networks. This supports the conclusion that CALEA does not otherwise limit or restrict the type of location information and related location information assistance capabilities that could and should be provided to law enforcement pursuant to lawful authorization. Thus, any reading of the statute that would preclude access to this information must be rejected.

3. The Commission Should Require Carriers to Provide All Signaling Information That Reveals the Location of a Mobile Handset That Is Reasonably Available to the Carrier Pursuant to Lawful Authorization

J-STD-025-B is deficient because it fails to specify that carriers provide all reasonably available signaling information that reveals mobile handset location information at the beginning and end of a communication that law enforcement is

74 *Id.*

legally authorized to receive.[75] J-STD-025-B contemplates the delivery to law enforcement of cell site location information only, regardless of the availability of more precise signaling information in a carrier's network, and more importantly, the presence of a court order authorizing law enforcement to receive more than just the cell site identifier. Thus, a carrier that employs J-STD-025-B will not have the capability to provision a CALEA-based intercept for any court order that authorizes law enforcement to receive something beyond cell site location information (i.e., longitude- and latitude-based location information).

When the Commission evaluated the location information capability in the original J-STD-025 standard, it considered whether carriers should be required to provide more precise location information for the subject's mobile handset based on the facts as they then existed.[76] At that time, the Commission declined to require carriers to

---

[75] For example, J-STD-025-B misleadingly states that location information will be "provided for established packet data sessions, when authorized, to identify location information *for* the intercept Mobile Station (MS)." See J-STD-025-B, Tables 18 and 20 (emphasis added). The use of the word "for" would allow the location information capability to be satisfied by providing the Base Station identification (i.e., the mobile cell site or tower identification), rather than the actual location of the mobile handset, even where the more accurate information is available in the carrier's network. MS or mobile handset longitude/latitude information is far more useful, and should therefore be provided pursuant to lawful authorization when reasonably available to a carrier.

[76] See id. at 16815 ¶ **43.** See *also* Comments of the New York City Police Department, CC Docket No. 97-213, at 7-8 (filed Dec. 18, 1998) (commenting that the location information that carriers should be required to provide is only that which is reasonably available to the carrier, and advocating that information used and/or available in a carrier's for purposes of providing overall service, maintenance, administration functionality, and call processing of individual calls should be considered to be

provide more precise location information, concluding that a more generalized location capability "[would] give [law enforcement agencies] adequate information."[77] The Commission went on to acknowledge, however, that its decision not to *require* the capability "does not preclude law enforcement agencies from requesting legal authority to acquire more specific location information in particular circumstances."[78]

Location identification technology has greatly advanced in its ability to precisely locate a wireless handset subscriber in the more than seven years since the Commission's *Third RDO* was issued. As a result of these advances, the types of signaling information reasonably available to carriers regarding handset location have changed dramatically. In particular, some carriers now use location technologies that result in more precise location information being generated by and reasonably available in their networks. These new technologies result in locations for the actual handsets that are more precise than those provided by older technologies – i.e., cell sites that would only allow extrapolation to general locations within a radius of miles.

These advances were spurred in part by the Commission's E-911 Phase II wireless services mandate, which requires wireless carriers to be capable of providing the precise latitude, longitude, and altitude location information for wireless

---

reasonably available),

[77] *See Third RDO* at 16816 ¶ 46. As discussed below, this has not generally been the case.

[78] *Id.*

subscribers' handsets. Many, if not most, carriers have deployed the **E-911** Phase II location capability in their networks in response to the Commission's mandate.[79] Several carriers have leveraged this investment in better location information capabilities and routinely use their **E-911** Phase II location information capability to assist them in other business and commercial operations, such as call completion and network management.[80] Carriers also have introduced new and improved wireless location service offerings to their subscribers.[81] CDMA2000 carriers and TIA already have developed and deployed a standard that enables wireless carriers to search for a subject's mobile handset location for commercial applications.[82] Thus, as a result of the

---

[79] 47 C.F.R. §§ 20.18(e), (g)(1)(v), (h). A list of the Commission's **E-911** wireless decisions can be found at the Commission's website at **http://www.fcc.gov/91l/enhanced/releases.html#ra** (last viewed May 14,2007).

[80] Indeed, carriers use longitude and latitude location information for the purpose of identifying the "origin" (i.e., geographic location) of the subscriber's handset not only for **E-911,** but also for network management and efficiency purposes. For example, carriers often use the more precise information to route calls through an alternate cell tower – rather than the "default" tower or one to which the call would ordinarily have been routed based on its proximity to the caller – in order to reduce the burden on a particular tower for network efficiency.

[81] See, *e.g.*, http://www.nextel.com/en/services/gps/mobile_locator.shtml (describing Sprint's wireless location-based services, including the ability to track individual users) (last viewed May 14, 2007). In addition, wireless carriers, in cooperation with state and local governments, are already testing traffic monitoring systems that utilize the wireless carriers' handset location information in order to reduce congestion. Matt Richtel, Tracking *Phones for Traffic* Reports, INT'L HERALD TRIB., Nov. **11,** 2005, at Finance, Pg. 19.

[82] TIA published a standard in early 2004 called TIA-881, which "enable[s] a wireless system to provide enhanced location services." See TIA, *TIA* Publishes *New* Standard TIA-881, Press Release, available at

E-911 mandate and consumer expectations and demand for new and better location-based wireless services, existing technology now routinely makes highly accurate geographical (latitude/longitude) wireless subscriber mobile handset location information "reasonably available" to carriers.[83]

In addition, although it is not relevant to whether Section 103 requires the location capability requested in this Petition, the Commission's conclusion in the *Third R&O* that a more generalized location capability would "give [law enforcement agencies] adequate information"[84] has not been borne out by subsequent experience. In

---

http://www.tiaonline.org/business/media/pressleases/legacy.cfm?parelease=04-65 (last viewed May 14, 2007).

[83] DOJ seeks to obtain, pursuant to proper legal authorization, all forms of signaling information that reveal the location of the subject's mobile handset at the beginning and the end of the communication only, and only when such location information is reasonably available to the carrier. DOJ's request that the Commission require carriers to be capable of providing more precise mobile handset location information (i.e., longitude/latitude) at the beginning and the end of each communication should in no way be construed as a request for a real-time tracking capability that would provide such information throughout the duration of the communication.

Such information will be "reasonably available" in many, if not most, carriers' networks by virtue of their compliance with the Commission's E-911 Phase II mandate. Given that other regulatory mandates already have directed carriers to deploy longitude/latitude-based mobile handset location capabilities, there would appear to be no reason not to leverage the existing presence of such capabilities with respect to CALEA. Such an approach would be consistent with CALEA's statutory purpose. In addition, just as the Commission's E-911 mandate calls for a phased-in approach whereby over time carriers would continue to improve the accuracy of the user information provided, so too should the accuracy of the location information provided to law enforcement pursuant to the requirements in Section 103 continue to improve over time as the result of technological advances and availability.

[84] *See Third R&O* at 16816 ¶ 46.

most cases, the more generalized cell site location information does not in fact provide law enforcement with "adequate" information, because it is frequently not usable in the manner in which the Commission anticipated. Both the operational challenges for law enforcement associated with the capability as adopted in the *Third R&O* and the technological advancements with respect to location identification in the last several years suggest that modifying the current location information capability as requested in this Petition is necessary and warranted in order to ensure that the location information capability's intended purpose is retained. Under the more generalized location information capability, carriers identify by cell site identifier the location of the cellular tower to which the handset is connected at the beginning and the end of a call. However, cell site information indicates only the general area in which a subject's mobile handset is located and cell sites often covers areas that are dozens or even hundreds of square miles, making it difficult for law enforcement to determine anything more than just the general vicinity of the handset.[85] Even worse, in some cases, the cell site location information that carriers provide to law enforcement is

[85] While many cell sites have a radius of one to three miles, some have a radius of as many as ten miles. Although a cell site with a one-mile radius will cover only approximately three square miles, a cell site with a three-mile radius will cover approximately 28 square miles, and a cell site with a ten-mile radius will cover approximately **314** square miles. While the combination of cell site plus sector identification serves to reduce the coverage area by approximately one-third, the coverage area would nonetheless remain quite large in many cases.

outdated and/or otherwise inaccurate.[86] Moreover, law enforcement has experienced problems with quickly and effectively correlating the cell site location information received from carriers to the physical location because there is no uniform carrier reporting mechanism for this information.

The Commission's conclusions in the original J-STD-025 deficiency proceeding should be read in light of their context. They do not preclude modifying the existing location information capability to require carriers to ensure access to all forms of signaling that reveal mobile handset location information that are now reasonably available to carriers. Moreover, a decision to adopt a rule requiring that all reasonably available signaling that reveals mobile handset location information be provided to law enforcement when authorized would not be inconsistent with the Commission's earlier position, given the technological advances and the operation of the capability in the years since the *Third ROO* was released. As discussed in this Petition, carriers' networks and services have evolved beyond their status at the time of the Commission's earlier decision. DOJ requests that the Commission require carriers to ensure law enforcement's ability to access all forms of signaling that reveal mobile handset location information pursuant to lawful authorization, when reasonably available to the carrier.

---

[86] The ability to accurately determine a subject's location is inherently tied to the quality of the mobile handset location information provided by the carrier. For the location information capability to work properly, carriers must regularly update tower site address location information and provide it to law enforcement. There have been times in the past, however, when carriers have not given law enforcement accurate location information for their cellular towers, rendering the cell site location

This will be the same signaling information that is already being made available by a number of carriers in connection with E-911 emergency services.[87]

In addition, in the original J-STD-025 deficiency proceeding, DOJ took the position in discussing the standard's location information capability that carriers need not have the capability to deliver more detailed location information in order to satisfy their obligations under CALEA.[88] DOJ also took the position that CALEA does not obligate carriers to design their networks to provide more extensive location information than what the standard itself specified.[89] These positions have not changed. DOJ's current request is that all signaling that reveals location information for a mobile handset at the beginning and the end of a communication be provided to law enforcement pursuant to lawful authorization *where such information is "reasonably*

---

information provided as part of the intercept solution useless.

[87] To the extent that the existence of such a capability may appear to the Commission to raise privacy concerns, the Commission may, as it has done previously, rely on the courts to regulate access to this information by law enforcement's proper showing of cause and need for such information in a particular case. See *Order on Remand* at 6927-28 ¶¶ 81-83 (concluding that whether a law enforcement agency is entitled to receive post-cut-through dialed digits under a particular type of legal authority is a legal question that should be left to the court that is considering a specific surveillance request).

[88] See Comments of the Department of Justice and the Federal Bureau of Investigation, CC Docket No. 97-213, at 74 (filed Dec. **18,** 1998). DOJ did note, however, that although CALEA does not *require* carriers to deliver more extensive location information than cell site information, CALEA does not *prohibit* carriers from doing so where carriers have designed their networks to generate such information, and law enforcement has been legally authorized to obtain such information. *Id.*

[89] *See id*

available" to a carrier. As discussed above, more accurate location information is now routinely generated by, and reasonably available in, many carriers' networks. Thus, carriers would not have to design (or redesign) their networks so as to create this information for the express purpose of complying with CALEA and providing it to law enforcement. Such information is already in carriers' networks and is being used by carriers and their customers. DOJ requests only that carriers be capable of providing this same reasonably available information when law enforcement is lawfully authorized in a specific matter to receive it.[90] Accordingly, DOJ requests that the Commission adopt a rule requiring carriers to be capable of providing all lawfully authorized mobile handset location information at the beginning and the end of a communication when such information is "reasonably available" to the carrier.

In addition, DOJ requests that the Commission require that a "toggle feature" be

---

[90] The Commission need only consider in the context of this proceeding whether the more precise/accurate mobile handset location information that would be provided by the modified capability is CII that should be provided to law enforcement pursuant to proper legal authorization where such information is reasonably available to the carrier. The Commission need not address – nor would it be appropriate for the Commission to address – the separate issue of what type of legal authorization law enforcement must obtain to be entitled to all forms of signaling information that reveals the location of a subject's mobile handset. For purposes of the Commission's analysis, the Commission can and should presume that law enforcement will have obtained the requisite legal authorization to enable it to request and receive such information from carriers. The Commission likewise should not fear that it will be opening the door to unauthorized collection of such information by requiring carriers to be capable of delivering it to law enforcement. J-STD-025-B itself makes the presentation of legal authorization by a law enforcement agency a precondition for a carrier's assistance with LAES. *See* J-STD-025-B § 1.1 (providing that "[a]s a precondition for a TSP's assistance with Lawfully Authorized Electronic Surveillance (LAES), [a law enforcement agency]

incorporated into this more precise location information capability to allow it to be turned "on" or "off" on a per-intercept basis consistent with the authority granted by a given court order.[91, 92] In order to avoid any confusion, DOJ recommends that the toggle

---

must serve a TSP with the necessary legal authorization").

[91] The Commission previously found – in the context of the dialed-digit extraction capability – that a toggle feature was a reasonable and appropriate way to address the issue of the differing types of legal authority for LAES that might be presented to carriers. See *Order on Remand* at 6930-31 ¶ 90. A similar "toggle" feature was adopted by the Commission and is included in J-STD-025-A for dialed-digit extraction. See 47 C.F.R. § 64.2203(c)(6) (now contained in 47 C.F.R. § 1.20007(b)(6)); ANSI/J-STD-025-A-2003, § 5.4.8.

[92] The current "location" capability in J-STD-025-8 identifies the "cell site" of the subject's mobile handset at the beginning and the end of a communication. The "Message Descriptions" section of J-STD-025-8 describes the various event messages that are relayed to law enforcement in connection with call/communication events. The event messages provided to law enforcement consist of a set of parameters, each of which is either "Mandatory," "Conditional," or "Optional." The event message parameter in J-STD-025-B for the delivery of location information is "Conditional," which means that location information is required to be provided only in situations where a condition (as defined in the standard) is met. Thus, J-STD-025-B currently requires the location information message field to be populated only where the delivery of location information is lawfully authorized and such information is reasonably available to the carrier. The standard contains a per-intercept toggle capability requirement to ensure the provision, or non-provision, of location information consistent with the type of lawful authority granted.

DOJ's request is not intended to replace the existing capability in the standard. Rather, it is intended to be a supplemental capability that would enable carriers to *also* provide this type of location information in addition to cell site where authorized and reasonably available. This would be accomplished by adding another "Conditional" location information message field that would be populated with the additional location information (i.e., longitude and latitude) where such information is lawfully authorized and is reasonably available to the carrier. Like the toggle feature already present in the standard to control the delivery or non-delivery of location information, including a per-intercept toggle capability for the additional location information message parameter would ensure the provision or non-provision of longitude and

feature for the more precise location information capability have a default setting of "off." Such a feature would help to better control delivery of the more precise and accurate location information to law enforcement by making the technical capability available and allowing the court to authorize, or not authorize, the delivery of such information on a case-by-case basis. This feature also would protect the privacy of communications not authorized to be intercepted by ensuring that law enforcement receives only the location information to which it is entitled by law.

V. The Security, Performance, and Reliability Capabilities Missing from J-STD-025-B Are Required by CALEA and Critical to Complying with Its Mandate

Security, performance, and reliability capabilities ensure the protection, completeness, and integrity of communications intercepts. Security-related capabilities measure and ensure the overall protection of a given interception. Performance- and reliability-related capabilities address the completeness and quality of the information delivered by a telecommunications carrier. J-STD-025-B lacks capabilities that adequately address these important CALEA-mandated requirements.[93]

---

latitude location information consistent with the type of authority granted. The inclusion of the additional field would enable a carrier to be capable of providing, on a per-intercept basis, whatever location information is lawfully-authorized and reasonably available to the carrier (i.e., no location information at all, cell site location information only, or both cell site and longitude/latitude location information).

[93] See 47 U.S.C. §§ 1002(a)(2)-(4), 1004.

A. Security, Performance, and Reliability Capabilities Are Required by CALEA Section **103**

1. Security

CALEA Section 103 requires telecommunications carriers to be capable of:

> facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects – (A) the privacy and security of communications and call-identifying information not authorized to be intercepted; and (B) information regarding the government's interception of communications and access to call-identifying information.[94]

Generally, this requires carriers to ensure that LAES can be implemented in a way that is transparent to (i.e., not detectable by) the intercept subject or other parties to the communication, and protect the fact of an interception and information related thereto. It also requires carriers to safeguard the assistance capabilities used to facilitate interception/LAES, and protect the packet data streams as they are delivered to law enforcement.[95]

It is also noteworthy that CALEA Section 105 and the Commission's security rules implementing that section require carriers to adopt internal security procedures regarding employee supervision, control, and access to communications content and CII

---

94 See *id.* § 1002(a)(4).

95 A capability that ensures the packet data streams are protected as they are delivered to law enforcement is critical because, to the extent that the CII is altered, mutilated, or manipulated, it would be rendered unusable, and law enforcement's access to call identifying information clearly would not be protected as required by Section 103(a).

obtained through LAES.[96] Together, Sections 103 and 105 prohibit improper carrier disclosure of LAES, and require carriers to protect LAES controls/assistance capabilities and the delivery of communications content and CII to law enforcement.[97]

2. Performance and Reliability

CALEA Sections 103(a)(2) and 103(a)(3) requires telecommunications carriers to be capable of:

> [E]xpeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to

---

[96] See 47 U.S.C. § 1004; 47 C.F.R. § 1.20003 (formerly 47 C.F.R. § 64.2103); *In the Mutter of Communications Assistance for Law Enforcement Act,* Report and Order, **14** FCC Rcd 4151 (1999).

[97] Section 105 and the Commission's security rules implementing that section require carriers to adopt internal system security and integrity policies and procedures for provisioning LAES. But the absence of Section 103 capabilities resident in the equipment that effectuate LAES pursuant to such carrier-adopted policies and procedures would render these policies and procedures useless. J-STD-025-A recognizes this very point in discussing both the Access Function and the Delivery Function, stating that each function typically includes "the ability . . . to protect (e.g., prevent unauthorized access, manipulation, and disclosure) intercept controls, intercepted call content and call-identifying information *consistent with [telecommunications service provider] security policies and practices." See* ANSI/J-STD-025-A-2003, §§ 5.3.1.1 and 5.3.1.2 (emphasis added).

In terms of safeguarding delivery of communications content and call identifying information to law enforcement, ensuring both the security of intercepted information sent from the Intercept Access Point ("IAP") to the Delivery Function ("DF"), and the security of intercepted information from the DF to the Collection Function ("CF") (in the case of carrier-provided buffering), is critical. To minimize the risk that such intercepted information might be improperly accessed or altered by unauthorized parties, the information provided via these delivery links should be kept physically or logically separate from other communications through the use of, for example, secure tunnels/virtual private networks ("VPN") – in order to protect communications content and CII delivered to law enforcement via the Internet.

> access call-identifying information that is reasonably available to the carrier. . . .;[98] and
>
> [D]elivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier. . . .[99]

CALEA obligates carriers to address quality of service concerns specifically for both the interception and the delivery of CII and communications content packets.[100] By explicitly including in CALEA an obligation as to the delivery of intercepted information to law enforcement, Congress unambiguously expressed its expectation that CALEA compliance would include addressing both the mechanisms for intercepting CII and communications content *and* the method by which such information is transmitted from the carrier to law enforcement.[101]

---

98 47 U.S.C. § 1002(a)(2).

99 *Id.* § 1002(a)(3).

100 *Id.* § 1002(a)(2)-(3).

101 DOJ's request that the security, performance and reliability of the delivery function be addressed should not be interpreted as a request for adoption of a standardized delivery interface. DOJ asks only that the Commission require that a carrier adequately address the security, performance, and reliability capability requirements in Section 103, which would include addressing the delivery of communications content and CII to law enforcement. The Commission has the authority to direct a standards-setting organization to adopt provisions that address the assistance capability requirements of Section 103 (e.g., security, performance, and reliability capabilities) without mandating a particular way of implementing the requirement.